The Anti-AI Scammer Playbook

Operational Framework for Detecting, Disrupted, and Defending Against Synthetic Fraud

1. Threat Matrix: Recognizing AI-Driven Attack Vectors

Modern cybercriminals leverage generative AI, deepfakes, and automated language models to engineer high-trust scams. Understanding the mechanism is the first line of defense:

Attack Vector	Technology Used	Primary Indicator
Voice Cloning & Vishing	Neural TTS / Audio Deepfakes	Unnatural pauses, robotic artifacts under stress, refusal to answer dynamic personal verification questions.
Synthetic Video / Facetime Spoofing	Real-time Generative GANs	Lighting inconsistencies around ears/hairline, minor frame jitter, slight latency mismatches.
AI Phishing & Social Engineering	Large Language Models (LLMs)	Impeccable multi-lingual grammar, highly tailored context mined from public profiles, rapid deployment speed.

2. Hardening Protocols & Counter-Measures

Phase A: Personal & Operational Authentication

- **Establish a Family/Team Safe Word:** Create a secure verbal pass-phrase known only to trusted circle members to bypass any urgent voice or video call requests for funds.
- **Out-of-Band Verification:** If a contact calls or messages claiming an emergency, hang up and initiate a separate, independent communication channel (e.g., calling them back on their known direct number).
- **Hardware-Backed Security:** Enforce physical security keys (such as a YubiKey managed behind a hardware-controlled USB switch) for all critical accounts to block token-hijacking and session-stealing attacks.

Phase B: Behavioral Interrogation Techniques

- **Trigger Non-Linear Logic:** Ask questions requiring shared historical context that an AI scraping public records cannot easily synthesize on the fly.
- **Disrupt the Pacing:** Force awkward conversational turns or ask the caller to touch their nose or move their hand across the camera to expose real-time generative video artifacts.

3. Incident Response & Reporting Pipeline

- **Immediate Isolation:** Revoke active session tokens, disconnect compromised machines from the network, and rotate master credentials immediately.
- **Financial Halt:** Contact banking institutions immediately to freeze wire transfers or flag fraudulent ACH requests.
- **Report to Authorities:** Submit detailed incident data to the FBI Internet Crime Complaint Center (IC3) or the FTC Scam Reporting Portal.